Attorney Docket No. 1046.1296

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Takeshi KASHIWADA

Application No.: UNASSIGNED | Group Art Unit: UNASSIGNED

Filed: July 21, 2003 | Examiner: To be Assigned

For: CONTROL SYSTEM HAVING DOWNLOAD FUNCTION

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant submits herewith a certified copy of the following foreign application:

Patent Application No. PCT/JP01/00356
Filed: January 19, 2001

It is respectfully requested that the applicant be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: July 21, 2003

By: _____
Gene M. Garner II
Registration No. 34,172

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

OP1102
US

日 本 国 特 許 庁

JAPAN PATENT OFFICE

別紙添付の書類は下記の出願書類の謄本に相違ないことを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００１年 １月１９日

出願番号
Application Number: ＰＣＴ／ＪＰ０１／００３５６

出願人
Applicant (s): 柏田 猛

２００３年 ３月 ２５日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証平 １５－５０００６８

受理官庁用写し

特許協力条約に基づく国際出願願書 0051727-1103

原本（出願用）- 印刷日時 2001年01月19日（19.01.2001）金曜日 14時53分10秒

0 0-1	受理官庁記入欄 国際出願番号.	PCT/JP01/00356
0-2	国際出願日	19.01.01
0-3	(受付印)	PCT International Application 日本国特許庁
0-4 0-4-1	様式-PCT/RO/101 この特許協力条約に基づく国際出願願書は、 右記によって作成された。	PCT-EASY Version 2.91 (updated 01.01.2001)
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記号	0051727-1103
I	発明の名称	ダウンロード機能を有する制御装置
II II-1 II-2	出願人 この欄に記載した者は 右の指定国についての出願人である。	出願人である (applicant only) 米国を除くすべての指定国 (all designated States except US)
II-4ja	名称	富士通株式会社
II-4en	Name	FUJITSU LIMITED
II-5ja	あて名:	211-8588 日本国 神奈川県 川崎市中原区 上小田中4丁目1番1号
II-5en	Address:	1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan
II-6	国籍（国名）	日本国 JP
II-7	住所（国名）	日本国 JP

特許協力条約に基づく国際出願願書 0051727-1103

原本（出願用）- 印刷日時 2001年01月19日（19.01.2001）金曜日 14時53分10秒

III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である（applicant and inventor）
III-1-2	右の指定国についての出願人である。	米国のみ（US only）
III-1-4ja	氏名（姓名）	柏田 猛
III-1-4en	Name (LAST, First)	KASHIWADA, Takeshi
III-1-5ja	あて名：	211-8588 日本国 神奈川県 川崎市中原区 上小田中4丁目1番1号 富士通株式会社内
III-1-5en	Address:	C/O FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan
III-1-6	国籍（国名）	日本国 JP
III-1-7	住所（国名）	日本国 JP
IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人（agent）
IV-1-1ja	氏名（姓名）	遠山 勉
IV-1-1en	Name (LAST, First)	TOYAMA, Tsutomu
IV-1-2ja	あて名：	103-0004 日本国 東京都 中央区 東日本橋3丁目4番10号ヨコヤマビル6階
IV-1-2en	Address:	Yokoyama Building 6th floor, 4-10, Higashi Nihonbashi 3-chome, Chuo-ku, Tokyo 103-0004 Japan
IV-1-3	電話番号	03-3669-6571
IV-1-4	ファクシミリ番号	03-3669-6573
IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人（additional agent(s) with same address as first named agent）
IV-2-1ja	氏名	松倉 秀実
IV-2-1en	Name(s)	MATSUKURA, Hidemi
V	国の指定	
V-1	広域特許 （他の種類の保護又は取扱いを求める場合には括弧内に記載する。）	---
V-2	国内特許 （他の種類の保護又は取扱いを求める場合には括弧内に記載する。）	JP US

特許協力条約に基づく国際出願願書　　0051727-1103

原本（出願用）- 印刷日時 2001年01月19日 (19.01.2001) 金曜日 14時53分10秒

V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。		
V-6	指定の確認から除かれる国	なし (NONE)	
VI	優先権主張	なし (NONE)	
VII-1	特定された国際調査機関(ISA)	日本国特許庁 (ISA/JP)	
VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	4	-
VIII-2	明細書	25	-
VIII-3	請求の範囲	6	-
VIII-4	要約	1	op1103pct abstract.txt
VIII-5	図面	8	-
VIII-7	合計	44	
	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-9	別個の記名押印された委任状	✓	-
VIII-10	包括委任状の写し	✓	-
VIII-16	PCT-EASYディスク	-	フレキシブルディスク
VIII-17	その他	納付する手数料に相当する特許印紙を貼付した書面	-
VIII-17	その他	国際事務局の口座への振込みを証明する書面	-
VIII-18	要約書とともに提示する図の番号	1	
VIII-19	国際出願の使用言語名:	日本語 (Japanese)	
IX-1	提出者の記名押印		
IX-1-1	氏名(姓名)	遠山 勉	

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	19.01.01
10-2	図面 :	
10-2-1	受理された	
10-2-2	不足図面がある	

特許協力条約に基づく国際出願願書 0051727-1103

原本（出願用）- 印刷日時 2001年01月19日（19.01.2001）金曜日 14時53分10秒

10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日（訂正日）	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	

明　細　書

ダウンロード機能を有する制御装置

技術分野

本発明は上位制御装置から制御機能の実行プログラムを受信して更新するダウンロード機能を有する制御装置に関し、特に正しく動作しないプログラムや不正なプログラムのダウンロードを防御するとともに、ダウンロードに失敗しても復旧を可能にするダウンロード機能を有する制御装置に関する。

背景技術

マイクロプロセッサの進歩及び普及により、各種周辺装置はプログラム制御化され、その機能も複雑になっている。また、電子商取引などの新しい技術の出現により，偽造や不正などに対するセキュリティが強く要求されるようになってきている。

例えば、銀行の窓口に代わって現金出納処理などを受け付ける自動機（現金自動支払機ＣＤまたは現金自動預け払い機ＡＴＭ）の暗証番号（ＰＩＮ）入力機能においては、従来はキーパッドの信号を自動機の制御部が直接処理し、暗証番号をそのままホストコンピュータシステムに送信していたが、現在ではセキュリティ構造の入力ユニットが暗証番号入力を受け付け、暗号化した暗証番号を自動機の制御部に渡す構成を採っている。これにより、物理的及び論理的な手法のいずれにおいても暗証番号を盗用することを困難にしている。

さらに、暗号化のアルゴリズムや暗号鍵の管理もより複雑でセキュリティの高い手法に移行している。

周辺装置に要求される機能の多くがソフトウェアによって実現され、しかも適宜機能の向上が要求されることから、物理的な部品交換などを必要とすることなく、周辺装置における制御機能の実行プログラムを更新するプログラムダウンロード手法が各種提案され、実施されている。

しかし、セキュリティの観点からは、不正なプログラムのダウンロードにより周辺装置、つまりダウンロード機能を有する制御装置（以下、ダウンロード制御

装置と記載することもある）の機能を停止したり、不正を実行可能にする危険が存在する。

また、故意の不正ではなく間違ったプログラムをダウンロードしたり、ダウンロードの途中で電源切断など予期せぬ障害が発生したために、ダウンロード制御装置が使用不能になる場合もある。

自動復旧機能はダウンロード制御装置の機能停止の防止には有効だが、作成した不正プログラムをダウンロードしてエラーが発生しても自動復旧後に再試行できるため、試行錯誤による不正プログラムの開発を助長する結果となる。

上位制御装置から送信されるプログラムにバージョン番号（版数）を設定し、ダウンロード制御装置に既に格納されているプログラムのバージョン番号と比較することにより、間違ったダウンロードを防止する手法がある。つまり、連続したバージョン番号以外はプログラムのダウンロードを受け付けないことにより、予期せぬダウンロードを検出して阻止する。

また、ダウンロードエラーを検出する技術としては、チェックサムやＢＣＣなどのチェックディジットを付加するエラー検出技術がよく知られている。

ダウンロード対象プログラムのねつ造や改ざんと、ダウンロードプログラムデータのエラーの検出とを目的とした発明として、特開平５－１７３８９２号公報「ファイルロード方式」がある。これはプログラムデータを暗号化して、その出力から生成したチェックディジットを使用するものである。

類似の発明として、特開平９－２８２１５５号公報「暗号認証機能の装備方法」がある。これは暗号化またはディジタル署名したプログラムを実行時にロード・復号化し、実行後はプログラムコードを消去するものである。

また、公開鍵でダウンロード対象プログラムを暗号化し、ダウンロードしたプログラムデータをダウンロード制御装置内の秘密鍵で復号する公開鍵暗号手法により、ダウンロード対象プログラムのセキュリティを確保できることは自明である。

ダウンロードに失敗した場合に機能を復旧する技術として、次の発明がある。つまり、複数のメモリに同一のプログラムを格納しておき、定期的にプログラムのチェックサムを計算してエラーを検出した場合、エラーの無いメモリからプロ

グラムをコピーする発明（特開平１１－１８４７０５号公報「ダウンロードプログラム補正装置及び方法」）、メモリを二つのエリアＡ及びエリアＢに分け、エリアＡの制御プログラムを実行している状態でエリアＢに新しい制御プログラムをダウンロードし、成功した場合のみエリアＢの制御プログラムを実行する発明（特開平１１－２６５２８２号公報「自動販売機の制御装置」）、及びダウンロードが成功したかどうかの識別情報を不揮発性メモリに書き込み、ダウンロードが成功していなければ起動時に再度ダウンロードを行う発明（特開２０００－１３７６０７号公報「デジタルテレビジョン受像機」）などである。

上述した従来技術において、ダウンロードモジュール（ダウンロード対象のプログラムデータなど）を暗号化しない技術では、ダウンロードモジュールを入手・解析して、ダウンロード制御装置のセキュリティ上の弱点を検出したり、改ざんしたダウンロードモジュールを作成したりすることが十分に可能である。

また、暗号化を用いる従来技術においては、暗号鍵の生成及び管理についての特別な手法は採用されていない。したがって、暗号鍵が入手されれば、暗号化されたダウンロードモジュールであっても解読及び改変されることになる。多数の暗号鍵（秘密鍵）をダウンロードモジュールに対応させて管理するのは煩雑であるため、暗号鍵自体の管理が不要なことが望まれる。

また、不正または事故によりダウンロードに失敗した場合、ダウンロード制御装置の機能を復旧させる従来技術では、不正なモジュールのダウンロードを試みて失敗しても復旧により同じ状態から再試行できるようになるため、不正モジュールの開発を容易にしてしまう。

内部のデータやプログラムを盗まれたり改ざんされたりしないように物理的かつ論理的な保護を行っているセキュリティモジュールについても、機能の修正や追加を容易にするためにプログラムダウンロード手法を採用したい。

しかし、セキュリティモジュールが簡単に解読可能であれば、このセキュリティモジュールの論理的弱点を暴露されたり、不正を行うべく改ざんされたりする危険がある。

また、版数の異なるダウンロードモジュールを間違ってダウンロードしたり、エラーを起こしたダウンロードプログラムを実行したりすることで、予期せぬ障

害を起こすことも考えられる。

そこで、暗号化セキュリティモジュールのダウンロード機能を有する制御装置においては、次のような要求を満足することが望まれる。

（１）版数が異なるなどの意図しないモジュール、データエラーを起こしたモジュールは受け付けない。

（２）ダウンロード途中でエラーを起こした（ダウンロード失敗）場合は、ダウンロードしたプログラムを決して実行しない。

（３）ダウンロードに失敗しても再度ダウンロードを行ってセキュリティモジュールの機能を復旧可能である。

（４）ダウンロードモジュールからプログラムを解読できない。

（５）正規のダウンロードモジュールを改ざんしてダウンロード可能なダウンロードモジュールを作成することができない。

（６）不正なダウンロード開発のためのダウンロードの試行錯誤を制限する。

（７）正規のダウンロードモジュールはキーワードの入力などを必要とせずにダウンロードできる。すなわち、キーワードなどの余分なセキュリティデータを必要としない。

（８）暗号鍵やキーワードなどの別途管理が必要な特別なデータを使用しない。

発明の開示

したがって、本発明の課題は、ダウンロード対象プログラムの解読や、ダウンロード可能な不正プログラムの作成・開発を困難にするとともに、誤ったダウンロードを防御することなどが可能な手法を提供することにある。

上記課題を解決するために、本発明のダウンロード機能を有する制御装置は、制御機能を実行するための実行プログラムデータを書き換え可能な状態で格納する第１の記憶手段と；

更新対象の新たな実行プログラムデータ及びモジュール識別情報を含むダウンロードモジュールを格納する第２の記憶手段と；

前記第１の記憶手段に格納されている前記実行プログラムデータと同一のプログラムデータと、前記モジュール識別情報とから作成された暗号鍵によって暗号

化された前記ダウンロードモジュールを受信して前記第２の記憶手段に格納する第１の制御手段と；

前記第１の記憶手段内の前記実行プログラムデータのデータと、前記第２の記憶手段内の前記ダウンロードモジュールのデータとから作成した暗号鍵によって前記ダウンロードモジュールを復号化し、前記ダウンロードモジュール中に暗号化されている格納開始アドレス、データ長及びチェックディジットが正当な値に平文化された場合、復号化された前記新たな実行プログラムデータで前記第１の記憶手段内の前記実行プログラムデータを置き換える第２の制御手段とを備える。

本発明の他のダウンロード機能を有する制御装置は、ダウンロード機能を起動後、予め定めた一定時間のみ、前記新たな実行プログラムデータを含む前記ダウンロードモジュールを受信可能とする第３の制御手段を更に備える。

本発明の他のダウンロード機能を有する制御装置は、前記ダウンロードモジュールの受信ができなくなった状態で特定のリセットコマンドを受信した場合、前記ダウンロード機能を再起動し、前記新たな実行プログラムデータを含む前記ダウンロードモジュールを受信可能とする第４の制御手段を更に備える。

本発明の他のダウンロード機能を有する制御装置は、前記ダウンロード機能の起動時に最初に実行され、前記第２の記憶手段に前記ダウンロードモジュールを格納するとともに、前記第１の記憶手段に格納された前記制御機能の実行プログラムデータを実行するローダを格納する第３の記憶手段を更に備える。

本発明の他のダウンロード機能を有する制御装置は、前記ローダが前記第１の記憶手段内の前記実行プログラムデータの全データに基づく演算結果から得られるチェックディジット値と、前記第１の記憶手段内の前記実行プログラムデータの特定アドレスのデータとが一致した場合、前記第１の記憶手段内の前記実行プログラムデータを実行可能とする第５の制御手段を更に備える。

本発明の他のダウンロード機能を有する制御装置は、前記ローダが格納されている前記第３の記憶手段に、前記第１の記憶手段に格納して実行可能な実行プログラムデータを格納しておき、

前記ローダが起動されて前記第１の記憶手段内の前記実行プログラムデータをチェックした結果、この実行プログラムデータを実行できないと判断した場合、

前記第３の記憶手段内の前記ローダ所有の前記実行プログラムデータを前記第１の記憶手段に格納して前記制御機能を回復する第６の制御手段を更に備える。

本発明の他のダウンロード機能を有する制御装置は、前記ローダが起動されて前記第１の記憶手段内の前記実行プログラムデータをチェックした結果、この実行プログラムデータを実行できないと判断した場合、前記第１の記憶手段を既知の状態に初期化して前記新たな実行プログラムデータの格納を可能にする第７の制御手段を更に備える。

本発明の他のダウンロード機能を有する制御装置は、前記ローダ所有の前記実行プログラムデータを前記第１の記憶手段に格納するまでの待ち合わせ時間を設定し、前記ローダによる前記第１の記憶手段の初期化と不正な実行プログラムデータを含む前記ダウンロードモジュールの前記第２の記憶手段への格納との繰り返しを制限する第８の制御手段を更に備える。

本発明の他のダウンロード機能を有する制御装置は、前記ローダにより前記第１の記憶手段を初期化するまでの待ち合わせ時間を設定し、前記ローダによる前記第１の記憶手段の初期化と不正な実行プログラムデータを含む前記ダウンロードモジュールの前記第２の記憶手段への格納との繰り返しを制限する第９の制御手段を更に備える。

本発明の他のダウンロード機能を有する制御装置においては、前記ダウンロードモジュールは、少なくとも前記モジュール識別情報としてのモジュール名称、モジュール作成日付及びモジュール版数と格納開始アドレスとを格納する固定長のヘッダ部と、

ブロック長とそれに対応する長さのデータとを格納する少なくとも１つのデータ部とから構成され、

前記データ部が実行プログラムデータ対応の実際のデータ長、格納開始アドレス、実行プログラムデータ、暗号化できるデータ長にするためのパッドデータ、及びこれらから生成するチェックディジットを含むブロックを暗号化されている。

この構成においては、前記第１の記憶手段内の前記実行プログラムデータのデータと、前記第２の記憶手段内の前記ダウンロードモジュールの前記モジュール識別情報のデータとから作成した暗号鍵によって前記ダウンロードモジュールを

復号化する。

上記ダウンロード機能を有する制御装置の各手法はダウンロード制御方法に適用できる。本発明のダウンロード制御方法は、制御機能を実行するための実行プログラムデータを書き換え可能な状態で第１の記憶手段に格納するステップと；

更新対象の新たな実行プログラムデータ及びモジュール識別情報を含むダウンロードモジュールを第２の記憶手段に格納するステップと；

前記第１の記憶手段に格納されている前記実行プログラムデータと同一のプログラムデータと、前記モジュール識別情報とから作成された暗号鍵によって暗号化された前記ダウンロードモジュールを受信して前記第２の記憶手段に格納するステップと；

前記第１の記憶手段内の前記実行プログラムデータのデータと、前記第２の記憶手段内の前記ダウンロードモジュールのデータとから作成した暗号鍵によって前記ダウンロードモジュールを復号化し、前記ダウンロードモジュール中に暗号化されている格納開始アドレス、データ長及びチェックディジットが正当な値に平文化された場合、復号化された前記新たな実行プログラムデータで前記第１の記憶手段内の前記実行プログラムデータを置き換えるステップとを備える。

図面の簡単な説明

図１は本発明の一実施の形態のダウンロード機能を有する制御装置の構成を示すブロック図である。

図２はダウンロードモジュールファイルの一例を示す図である。

図３はダウンロードモジュールファイルの他の例を示す図である。

図４はメモリマップの構成を示す図である。

図５はダウンロード処理の概要を説明するためのフローチャートである。

図６はダウンロード処理の詳細を説明するためのフローチャートである。

図７はダウンロード処理の詳細を説明するためのフローチャートである。

図８はダウンロード処理の詳細を説明するためのフローチャートである。

発明を実施するための最良の形態

次に、本発明の実施の形態について図面を参照して説明する。

〔ダウンロード機能を有する制御装置の構成〕

本発明の一実施の形態におけるダウンロード機能を有する制御装置（ダウンロード制御装置）の構成を示す図１を参照すると、このダウンロード制御装置１においては、制御部（ＣＰＵ）２は、通常状態では、メモリ部３のダウンロード部（実行プログラム格納領域）７に格納されているプログラムコード（プログラムデータと記載することもある）を実行する。

また、ＣＰＵ２は通信インターフェース４及び通信回線５を経由して図示省略の上位制御装置（ホストコンピュータ）からコマンド及びプログラムデータを受信し、処理結果を上位制御装置に送信したり、入出力部（Ｉ／Ｏ）９を制御する。

ＣＰＵ２がメモリ部３の実行プログラム格納領域７に格納されているプログラムコードを書き換える場合は、メモリ部３のローダ部６に格納されているプログラムコード（ローダ部コード）４３を実行する。

メモリ部３はローダ部６、実行プログラム格納領域７及び作業領域８から構成されている。ローダ部６、実行プログラム格納領域７及び作業領域８は、同一のメモリ素子の記憶領域を論理的に分割して構成するか、異なるメモリ素子をそれぞれ対応させて構成することが可能である。

ＣＰＵ２は通信インターフェース４経由でダウンロード対象のプログラムデータを受信してメモリ部３の作業領域８に格納し、後に詳述するようにエラーがなければ、実行プログラム格納領域７のプログラムデータを書き換えるためのコード（書き込みルーチン）を実行する。この書き込みルーチンはメモリ部３のローダ部６に格納されているが、メモリ部３の構成によっては、書き込みルーチンを作業領域８に複写して実行する。

このダウンロード制御装置１は、Ｉ／Ｏ９として、顧客が入力する暗証番号（ＰＩＮ）を暗号化して入出力インターフェース（図示省略）に出力するセキュリティキーボードなどを備える。

このダウンロード制御装置１は暗号化アルゴリズムとして既存のいずれかの手法を採用可能であるが、例えば６４ビットの鍵と６４ビットのイニシャルベクタとを用いたＤＥＳ－ＣＢＣ（サイファ・ブロック・チェイニング・モード）アル

ゴリズムを適用できる。

なお、ダウンロード制御装置１は、例えばＣＤやＡＴＭなどの自動機やクレジット照会端末（ＣＡＴ）もしくはそれらの暗証番号（ＰＩＮ）処理部などであるが、これらの装置としての基本機能自体については、本発明の範囲外であるためここでは説明を省略する。

〔ダウンロードモジュールファイルの構成〕

図２は単純なダウンロードモジュールファイル２０の一例を示す。ここで、ダウンロードモジュールとは、外部からアクセス可能なファイルや、通信データの状態にあるダウンロード対象のプログラムデータを含むモジュールである。

ダウンロードモジュールファイル２０はヘッダ部２１及びデータ部２２から構成されている。このダウンロードモジュールファイル２０においては、固定長のヘッダ部２１はファイル自体の管理とエラーチェックとのために、モジュール名称、モジュール作成日付、モジュール版数及び格納開始アドレスなどのプログラムモジュール識別情報２３の格納領域を有する。

また、データ部２２はエラーチェックのために、格納データ（プログラムデータ）２４に付加する格納開始アドレス、データ長及びチェックディジットの格納領域を有する。

チェックディジットは格納開始アドレスとデータ長と格納データ２４とのすべてから求める。すべてのデータを加算して１または２の補数をとるチェックサムがチェックディジットを求める場合の代表的な手法である。

図３はダウンロードモジュールファイル２０の他の例を示す。図２に示すダウンロードモジュールファイル２０と異なるのは、データ部２２が送信単位に対応する複数の本体部（１，２…Ｎ）に分割されていて、ヘッダ部２１及び各本体部のそれぞれにおいて通信エラーチェックを行えるようにしてある点である。

また、ＤＥＳ－ＣＢＣなどの固定ブロック長データを処理する暗号化アルゴリズムに対応するために、データ部２２の各本体部の実際のプログラムデータの後ろにデータ長を合わせるための、つまり暗号化できるデータ長にするためのパッドデータを付加する。

したがって、このダウンロードモジュールファイル２０はヘッダ部２１と複数

の本体部を含むデータ部２２とから構成されている。このダウンロードモジュールファイル２０においては、固定長のヘッダ部２１はファイル自体の管理とエラーチェックとのために、モジュール名称、モジュール作成日付、モジュール版数及び格納開始アドレスと、更にチェックディジットなどとのプログラムモジュール識別情報２３の格納領域を有する。

また、データ部２２の各本体部はエラーチェックのために、格納データ（プログラムデータ）２４に付加するブロック長、格納開始アドレス、データ長（実際のプログラムデータ長）、及びチェックディジットの格納領域を有する。

チェックディジットは、上記と同様に、例えばすべてのデータを加算して、１または２の補数をとるチェックサム手法を採る。

図３に示すダウンロードモジュールファイル２０のヘッダ部２１及びデータ部２２の具体例は次のとおりである。

ヘッダ部２１：

```
char    moduleName[16] = "PATENTED MODULE";     ……モジュール名称
char    moduleDate[10] = "2000-07-07";          ……モジュール作成日付
char    moduleVersion[4] = "AA01";              ……モジュール版数
ADDR    loadAddress;                            ……格納開始アドレス
CHKDG   checkDigit;                             ……チェックディジット
/* その他必要に応じて追加 */
```

データ部２２の暗号化前の本体各部：

```
int     blockSize = sizeof(ADDR) + sizeof(int) +DATASIZE_n
                  + PADSIZE_n + 1;              ……ブロック長
ADDR    loadAddress;                            ……格納開始アドレス
int     dataSize = DATASIZE_n;                  ……データ長
char    data[DATASIZE_n];                       ……データ（格納データ２４）
char    padData[PADSIZE_n];                     ……パッドデータ
char    checkDigit;                             ……チェックディジット
/* 暗号化できるｂｌｏｃｋＳｉｚｅになるようＰＡＤＳＩＺＥ＿ｎを決める
（ＤＥＳ－ＣＢＣ暗号化では、８の倍数） */
```

図２及び図３のいずれのダウンロードモジュールファイル２０とも、データ部２２はダウンロード対象装置内のメモリ部の実行プログラム格納領域内に格納されているのと同一のプログラムデータと、プログラムモジュール識別情報とを基に作成した暗号鍵を用いて暗号化されている。図２及び図３に示したデータ部２２の内容は暗号化される前のものである。

後に詳述するが、ダウンロード制御装置１が上位制御装置からのプログラムデータのダウンロードを実行する場合、図２及び図３に示すダウンロードモジュールファイル２０を通信インターフェース４経由で一括または分割して受信する。

いずれのファイル形態においてもダウンロードモジュールファイル２０のデータ部２２のうちの格納データ２４が、メモリ部３の実行プログラム格納領域７に格納される。

ダウンロード対象のダウンロードモジュールファイル２０をメモリ部３の作業領域８に受信したダウンロード制御装置１は、メモリ部３の実行プログラム格納領域７に既に格納されている旧プログラムデータと、受信したファイルのヘッダ部２１のプログラムモジュール識別情報２３とに基づいて作成した暗号鍵を用いて、受信したファイルのデータ部２２を復号化し、格納開始アドレス、データ長及びチェックディジットが正当であれば、新プログラムデータを実行プログラム格納領域７に格納する。

〔メモリマップの構成〕

図４はダウンロード制御装置１におけるメモリ部３のメモリマップ４０の一例を示している。

メモリマップ４０において、メモリ部３のローダ部６及びダウンロード部（実行プログラム格納領域）７は、ダウンロード制御装置１の電源が切断された場合でもその記憶内容が破壊されない不揮発性素子または回路構成のメモリ（例えば、フラッシュＲＯＭ）から構成される。作業領域８は書き込み及び読み出しを常時繰り返すのに適したメモリ素子（ＲＡＭ）から構成される。

ここでは、ＣＰＵ２はリセット及び例外処理の各ルーチンアドレスを０（０００：１６進数）番地から始まるメモリアドレス空間に持つタイプを想定している。リセット時の実行開始アドレスはリセット割込みベクタ４１により指定され

るローダ部コード４３であり、装置電源投入時及びリセット時にはここから実行が開始される。

また、その他割込みベクタ４２の実行開始アドレスは作業領域８の先頭に配置したジャンプ命令からなる割込み中継ベクタ４８にジャンプするように設定してある。

このメモリマップ４０におけるローダ部６のリセット割込みベクタ４１は、ダウンロード制御装置１への電源投入または装置リセット後に、ＣＰＵ２が最初に実行するメモリ部３の番地を格納している。本例では、ローダ部コード４３から実行を開始する。ダウンロードの失敗などによって制御装置１が復旧不能に陥らないように、このベクタ領域はＣＰＵ命令により書き換わることがないメモリ（ＲＯＭ）に配置する。

その他割込みベクタ４２は、リセット割込み以外の割込み時、割込み要因毎にＣＰＵ２が実行する番地を格納する。この実施形態では、効率的な通信のために通信インターフェース４からの割込みを使用する。割込み処理は、ダウンロード処理中はローダ部コード４３で行い、装置アプリケーション実行中はアプリケーション部すなわちダウンロード部コード４６で行う必要がある。

ＣＰＵ２のアーキテクチャからすると、リセット割込みベクタ４１とその他割込みベクタ４２とは、通常連続したメモリアドレスに配置される。リセット割込みベクタ４１をＲＯＭに配置すれば、その他割込みベクタ４２もＲＯＭに配置され、ＣＰＵ命令により書き換えることはできない。

このため、その他割込みベクタ４２は割込み中継ベクタ４８と呼ばれる書き換え可能なＲＡＭ領域の命令を実行するように設定し、そこからローダ部コード４３またはダウンロード部コード４６にジャンプするように設定する。

ローダ部コード４３は、後に詳述するダウンロード処理を行うＣＰＵコードを格納するための領域である。ダウンロードの失敗などによってダウンロード制御装置１が復旧不能に陥らないように、この領域はＲＯＭに配置する。

ダウンロード部初期コード４４は、ダウンロード部７に展開して実行するためのプログラムコードである。ダウンロード部コード４６が正しくないと判定された場合に、ダウンロード部７に展開され、ダウンロード制御装置１の基本機能を

復旧する。その目的から、本領域はＲＯＭに配置する。

ローダ部チェックディジット４５は、リセット割込みベクタ４１、その他割込みベクタ４２、ローダ部コード４３、及びダウンロード部初期コード４４の内容が正しいかどうかをチェックするためのデータである。簡単かつ一般的な手法として、ローダ部６を構成するＲＯＭ全体のデータの加算値を用いるチェックサムがある。

ダウンロード部７のダウンロード部コード４６は、ダウンロード制御装置１のアプリケーション処理コードを格納する領域である。この領域はダウンロード処理により書き換えられる。ダウンロード部チェックディジット４７は、ダウンロード部７のデータが正しいかどうかをチェックするためのデータである。

作業領域８の割込み中継ベクタ４８は、ＣＰＵ割込み処理ルーチンへのジャンプ命令を格納する領域である。データ領域４９及びスタック領域５０は、ローダ部６の命令コード４３，４４またはダウンロード部７の命令コード４６の実行に必要な作業領域である。

〔暗号鍵データ生成コード〕

図３に示すダウンロードモジュールファイル２０と、図４に示すメモリマップ４０とに基づいて、ダウンロード対象のプログラムデータの暗号鍵を生成するアルゴリズムの一例を次に示す。

この例では、６４ビットの鍵をハッシュ技法を使わずに直接的に２つ生成している。この場合、暗号化アルゴリズムとしては、ＤＥＳ－ＣＢＣが適しているが、暗号強度とコードサイズや処理速度との兼ね合いで、生成する暗号鍵サイズと生成アルゴリズム及び暗号化アルゴリズムとを選択可能である。

暗号鍵データ生成コード：

```
char key1[8], key2[8];
#define MEM(address)  *(char *)(address)    /* get the byte at address */
void getkey(void)
{
     key1[0] = moduleDate[2];     /* year part */  ……モジュール作成日付
     key1[1] = moduleDate[3];
```

```
    key1[2] = moduleDate[5];     /* month part */ ……モジュール作成日付
    key1[3] = moduleDate[6];
    key1[4] = moduleDate[8];     /* day part */   ……モジュール作成日付
    key1[5] = moduleDate[9];
    key1[6] = moduleVersion[1]; /* version */     ……モジュール版数
    key1[7] = moduleVersion[3];

    key2[0] = MEM(0x8001);       /* memory data at address 0x8001 */
    key2[1] = MEM(0x8002);
    key2[2] = MEM(0x9800);
    key2[3] = MEM(0x9801);
    key2[4] = MEM(0x9802);
    key2[5] = MEM(0x9803);
    key2[6] = MEM(0xFFFE);
    key2[7] = MEM(0xFFFF);
}
```

上位制御装置において、ダウンロードモジュール、つまりダウンロード対象の暗号化セキュリティモジュールを作成する場合は、既にダウンロード制御装置１に書き込まれている旧プログラムデータと、これからダウンロードしようとする新プログラムデータ対応のプログラムモジュール識別情報２３とから暗号用の暗号鍵を生成する。

暗号化セキュリティモジュールを受信したダウンロード制御装置１では、自装置に格納されている旧プログラムデータと受信した新プログラムデータとから復号用の暗号鍵を生成する。このような暗号鍵生成方法により、後述するように多くの利点が生まれる。

〔ダウンロード機能を有する制御装置の動作〕

（各種動作例）

次に、上述したダウンロード制御装置１の動作を説明する。

（１）図１，図２，図３及び図４を併せ参照すると、上述したダウンロード制

御装置１においては、書き換え可能なメモリに制御機能の実行プログラムを格納して実行する。ダウンロード制御装置１は、実行プログラム格納領域７内のプログラムデータと、それ以外のデータであるプログラムモジュール識別情報２３とを合成して作成した暗号鍵により暗号化された新たな実行プログラムを含むダウンロードモジュールファイル２０を通信インターフェース４を経由して上位制御装置から受信する。

この後、ダウンロード制御装置１は、実行プログラム格納領域７内の旧プログラムデータと、受信したプログラムモジュール識別情報２３とを合成して作成した暗号鍵で復号化し、受信したダウンロードモジュールファイル２０のデータ部２２中に暗号化されている格納開始アドレス、データ長、及びチェックディジットが正当な値に平文化された場合にのみ、復号化されたプログラムデータでメモリ部３の実行プログラム格納領域７内の実行プログラムを置き換える（書き換える）。以後、ダウンロードした新しいプログラムコードを実行する。

この動作を行う構成のダウンロード制御装置１においては、ダウンロードモジュールファイル２０が暗号化されているため、そのままでは内容を知られることがない。暗号鍵の生成にはダウンロード制御装置１に格納されているプログラムコード４６が必要であるが、ダウンロード制御装置１に格納されているプログラムコード４６が知られることがないようにする手段は既知である。

上位制御装置では、ダウンロードするプログラムモジュール識別情報２３から暗号鍵を生成するため、たとえ全く同一のプログラムモジュールであってもプログラムモジュール識別情報２３が異なれば、暗号化されたダウンロードモジュールのデータは全く異なったものとなり、暗号を解読してダウンロードモジュールファイル２０自体からプログラムコード４６を知ることを一層困難にしている。

ダウンロード対象のプログラムデータの格納開始アドレス、データ長、及びチェックディジットを暗号化して付加しているため、通信エラーや改ざんなどでデータの一部が変更／追加／削除された場合、復号化されたプログラムデータの格納開始アドレスの妥当性、データ長、またはチェックディジットの計算結果の各チェック時のどれかでエラーとなり、正常にダウンロードできない確率を極めて高くすることができる。

上位制御装置では、ダウンロードしようとしているダウンロード制御装置１に既に格納されているプログラムコード４６から、厳密には上位制御装置が持っているこのプログラムコード４６の原本またはコピーから暗号鍵を生成するため、異なるプログラムコード４６を格納したダウンロード制御装置１用に作成されたダウンロードモジュールファイル２０をダウンロードすると、ダウンロード制御装置１が自分で持っているプログラムコード４６から生成した暗号鍵ではエラーとなり、正常にダウンロードできない確率を極めて高めることができる。

このように意図しないダウンロードが成功する確率が極めて低いため、ダウンロード実行時に操作者にキーワードの入力を要求し、キーワードが一致しない場合は、ダウンロードを実行しないようにするなどのセキュリティ追加が不要である。また、ＲＳＡなどの非対象鍵（公開鍵と秘密鍵）方式の暗号アルゴリズムを用いる必要がないため、高速処理が可能である。

（２）上記基本動作の構成において、ダウンロード処理プログラム（ローダを含む）を起動後、予め定めた一定時間のみ新たな実行プログラムデータの受信が可能であり、一定時間経過後には装置本来の基本機能のみが実行可能となるようにダウンロード処理プログラムを構成する。

これにより、装置起動またはリセット後の限られた時間内にダウンロードが開始されない場合、ダウンロードモジュールファイル２０のダウンロードができないため、意図しないダウンロードが行われることを防止できる。

（３）また、プログラムデータの受信ができなくなった状態で、上位制御装置から特定のリセットコマンドを受信すると、ダウンロード処理プログラムを再起動し、プログラムデータの受信を可能にする。つまり、ダウンロード処理プログラム起動後、一定時間だけダウンロードを受け付け、その後はリセットコマンドによってダウンロード処理プログラムを再起動することが可能となるようにダウンロード処理プログラムを構成する。

これにより、ダウンロードを開始したい時は、リセットコマンドを発行することでいつでもダウンロードを開始することができる。上位制御装置のソフトウェアが起動後、ダウンロードを開始できるようになるまでにはかなりの時間がかかるため、ダウンロード制御装置１と上位制御装置とを同時に起動して確実にダウ

ンロードを行うためには、ダウンロード制御装置１を起動後、ダウンロード可能な時間を十分に長くしておく必要がある。

セキュリティ上、この間ダウンロード制御装置１は通常機能を実行しないことが望ましいが、そうすると直ぐに運用を開始することができない。リセットコマンドによりダウンロード制御装置１を再起動してダウンロードを開始することで、ダウンロード制御装置１を起動（再起動）後、ダウンロード可能な時間を短縮して、装置起動から運用開始までの無用な待ち時間を無くすことができる。

再起動してからダウンロードを開始するため、運用基本機能の影響を受けずに、ダウンロードを行うようにダウンロード処理プログラムを構成することが容易であり、信頼性が向上する。

（４）受信した実行プログラムデータを格納するメモリ（実行プログラム格納領域７）とは別のメモリ素子またはメモリ領域（ローダ部６）に、新たなプログラムデータを受信・格納するダウンロード処理プログラムのローダを格納しておき、装置起動時はこのローダが最初に実行され、装置本来の基本機能を実現するプログラムは専用メモリまたはメモリ領域（実行プログラム格納領域７）に格納されていて、ローダから実行されるように構成する。

つまり、実行プログラムを格納するメモリ空間を２つに分け、一方は起動時／リセット時に実行され、かつダウンロードを行うローダ部６とし、不揮発性かつ書き換え不可能または書き換え禁止とする。他方の実行プログラム格納領域（ダウンロード部）７は書き換え可能かつ不揮発性で、ダウンロードされた装置基本機能プログラムを格納するものとする。これらは互いに物理的に分離したメモリ素子で構成するか、一つのメモリ素子をアドレス範囲により分割する。

このように、起動からダウンロードを行うまでの部分のコードを格納するメモリと、ダウンロードにより書き換えるメモリとを分離することにより、ダウンロードに失敗してもダウンロード機能を喪失することはない。

（５）実行プログラム格納領域７内の全プログラムコード４６を使った演算結果から得られるチェックディジット４７の値が、実行プログラム格納領域７の特定アドレスのプログラムコード４６と一致した場合のみ、ローダは実行プログラム格納領域７内のプログラムを実行する。

つまり、上記動作（４）において、ローダがダウンロードを行なわなかった場合、実行プログラム格納領域７のプログラムコード４６を実行するが、実行プログラム格納領域７の全体についてチェックディジット４７の計算を行い、エラーとなった場合は実行せず、すべての基本機能を停止するようにローダ部のダウンロード処理プログラムを構成する。

これにより、ダウンロードに失敗して中途半端なプログラムコード４６が実行プログラム格納領域７に残った場合にそのプログラムコード４６を実行してしまって問題を起こすことを防止できる。

（６）ローダと同じメモリ素子またはメモリ領域に、実行プログラム格納領域７に格納し実行できるプログラムコード（ダウンロード部初期コード４４）を格納しておき、ローダが起動され実行プログラム格納領域７のプログラムコード４６をチェックした結果、実行プログラム格納領域７のプログラムコード４６を実行できないと判断した場合、ローダ側が持っているダウンロード部初期コード４４を実行プログラム格納領域７に格納して、装置の基本機能を回復する。

つまり、上記動作（５）において、実行プログラム格納領域７のプログラムコード４６がエラーであると判定された場合、ローダがローダ部６に予め格納されているコード４４を用いて実行プログラム格納領域７にプログラムコード（ダウンロード部コード）４６を書き込み、以後装置基本機能の一部または全部を実行可能とするようにローダ部６のダウンロード処理プログラムを構成する。

これにより、ダウンロードに失敗した場合でも、プログラムコード４６を自動的に自己復旧し、装置の基本機能を回復することができる。ただし、最新のプログラムコード４６ではないため、若干の制限が生じる可能性がある。

（７）ローダが起動され、実行プログラム格納領域７のプログラムコード４６をチェックした結果、実行プログラム格納領域７のプログラムコード４６を実行できないと判断した場合、実行プログラム格納領域７を既知の状態に初期化することにより、新たな実行プログラムデータの受信・格納を確実に行えるようにしている。

つまり、上記動作（５）において、実行プログラム格納領域７のプログラムコード４６がエラーであると判定した場合に、ローダが実行プログラム格納領域７

をクリアして既知の状態に戻すように、ローダ部６のダウンロード処理プログラムを構成する。

ダウンロードに失敗して中途半端なプログラムコード４６が実行プログラム格納領域７に残った場合、そのままでは復号化に用いるプログラムコード４６が不明になって、ダウンロード可能なダウンロードモジュールファイル２０を作成することができなくなる。既知の状態にクリアすることにより、その状態に対応したダウンロードモジュールファイル２０を作成し、ダウンロードすることを可能にする。

（８）ローダがローダ側の持っている実行プログラムデータ、つまりローダ部６のダウンロード部初期コード４４を実行プログラム格納領域７に格納する前に、相当な時間、何もせずにいることにより、実行プログラム格納領域７の初期化と不正な実行プログラムコードの格納との繰り返しを制限する。

つまり、上記動作（６）におけるエラー判定から実行プログラム格納領域７のコード４６の初期化開始まで所定の時間、何もしないようにローダ部６のダウンロード処理プログラムを構成する。

これにより、ダウンロードモジュールファイル２０の解読や不正ダウンロードモジュールファイル２０の作成の目的で試験的なダウンロードを繰り返し行なおうとしても、ダウンロード失敗の度に相当な時間、待たなくては次の試行ができない。このために、そのような攻撃を行う意欲を削ぎ、攻撃が成功する可能性を殆ど無くすことができる。

（９）上記動作（７）において、ローダが実行プログラム格納領域７を初期化する前に、相当な時間、何もせずにいることにより、実行プログラム格納領域７の初期化と不正な実行プログラムコードの格納との繰り返しを制限する。つまり、エラー判定から実行プログラム格納領域７のクリア実行まで、所定の時間、何もしないようにローダ部６のダウンロード処理プログラムを構成する。

これにより、上述した繰り返し攻撃を行う意欲を削ぎ、攻撃が成功する可能性を殆ど無くすことができる。

（１０）ダウンロードモジュールファイル２０は、プログラムモジュール識別情報２３としてのモジュール名称、モジュール作成日付、モジュール版数及び格

納開始アドレスを格納する固定長のヘッダ部２１と、ブロック長とそれに対応する長さのデータとからなる複数のデータ部２２とから構成されている。

このデータ部２２においては、格納開始アドレス、実際のデータ長、格納データ（プログラムデータ）、暗号化できるデータ長にするためのパッドデータ、及びこれらから生成するチェックディジットとを有するブロックを暗号化してある。

このファイル２０を受信したダウンロード制御装置１は、実行プログラム格納領域７に既に格納されているプログラムデータと、受信したファイル２０のヘッダ部２１のプログラムモジュール識別情報２３とに基づいて、受信したファイル２０のデータ部２２を復号化し、格納開始アドレス、データ長及びチェックディジットが正当であれば、受信したファイル２０の新プログラムデータを実行プログラム格納領域７に格納する。

つまり、ダウンロードモジュールファイル２０のヘッダ部２１にダウンロードモジュール識別情報２３として、モジュール名称、モジュール作成日付、及びモジュール版数などを格納する。

ダウンロード対象のプログラムデータは通信エラーチェックに適したサイズに分割し、それぞれに格納開始アドレス、データ長、採用した暗号化アルゴリズムが要求するデータ長に合わせるためのパッドデータ、これらとダウンロード対象プログラムデータとから計算されるチェックディジットを付加してデータブロック（データ部）２２として暗号化し、ヘッダ部２１に続けてそれぞれのデータブロック長と暗号化したデータ部２２を連続してダウンロードモジュールファイル２０を構成する。

暗号化に用いる暗号鍵は、ダウンロード対象のダウンロード制御装置１の実行プログラム格納領域７に現在格納されているプログラムコード４６と、ダウンロードモジュールファイル２０のヘッダ部２１のダウンロードモジュール識別情報２３とから作成する。

暗号鍵の一部にダウンロードモジュール識別情報２３が含まれるため、誤ったダウンロードモジュールファイル２０をダウンロードしようとしても暗号鍵が一致しないため、復号化した段階でエラーとなり、誤ってダウンロードしてしまうことを防止できる。また、ダウンロード対象のデータ部２２を分割することによ

り、ダウンロードの必要の無いメモリ領域に対応したデータ部２２を省略することができ、ダウンロード所要時間を短縮できる。

（ダウンロード処理の概要）

次に、図１，図２及び図５を併せ参照して、ダウンロード処理の概要について説明する。図５は、図１に示すダウンロード制御装置１が上位制御装置から図２に示す形態のダウンロードモジュールファイル２０をダウンロードする場合の処理手順を示す。

この場合、ダウンロード対象のダウンロードモジュールファイル２０は上位制御装置において上記暗号化アルゴリズムによって暗号化されている。ダウンロード制御装置１においては、ＣＰＵ２はメモリ部３のローダ部６に格納されているダウンロード処理プログラムコードを実行する。

ＣＰＵ２は通信回線５及び通信インターフェース４を通して上位制御装置から暗号化されたダウンロードモジュールファイル２０を受信して、メモリ部３の作業領域８に格納する（処理手順Ｓ５０）。ＣＰＵ２は、通信エラーがなければ、受信したダウンロードモジュールファイル２０のヘッダ部２１をチェックする（Ｓ５１）。

正常である場合、復号用暗号鍵が生成される（Ｓ５２）。この復号用暗号鍵は実行プログラム格納領域（ダウンロード部）７の特定アドレスに既に格納されている旧プログラムデータと、受信したファイル２０のヘッダ部２１の一部のデータとから生成される。ここでは、ヘッダ部２１の一部のデータとして、プログラムモジュール識別情報２３のうちのモジュール名称、モジュール作成日付及びモジュール版数を利用する。

次に、ＣＰＵ２はファイル２０のデータ部２２を復号し（Ｓ５３）、復号化した格納開始アドレスとデータ長とが有効か否かを判断する（Ｓ５４）。有効である場合、復号化されたデータ部２２のチェックディジットが算出される（Ｓ５５）。

ＣＰＵ２は、算出したデータ部２２のチェックディジットと、受信したファイル２０のデータ部２２中のチェックディジットとが、一致するか否かを判断する（Ｓ５６）。チェックディジットが一致する場合、メモリ部３の作業領域８に格

納している受信プログラムデータを実行プログラム格納領域７に書き込む（Ｓ５７）。

（ダウンロード処理の詳細）

続いて、図１，図３，図４，図６，図７及び図８を併せ参照して、ダウンロード処理の詳細について説明する。図６，図７及び図８は、図１に示すダウンロード制御装置１が上位制御装置から図３に示す形態のダウンロードモジュールファイル２０をダウンロードする場合の処理手順を示す。

この場合、ダウンロード対象のダウンロードモジュールファイル２０は上位制御装置において上記暗号化アルゴリズムによって暗号化されている。ダウンロード制御装置１においては、ＣＰＵ２はメモリ部３のローダ部６に格納されているダウンロード処理プログラムコードを実行する。

ダウンロード制御装置１に電源が投入されると、ＣＰＵ２は全ての割込みデバイスからのアクセスを停止する（図６中の処理手順Ｓ６０）。そして、ＣＰＵ２はメモリ部３のローダ部６のデータから計算したチェックサムと、メモリ部３のローダ部６のローダ部チェックディジット４５とを比較して、ローダ部６の内容が正しい状態にあることを確認する（Ｓ６１）。

続いて、作業領域８へのデータの書き込みと書き込んだデータの読み出しが正常に行えることを確認する（Ｓ６２）。手順Ｓ６１またはＳ６２においてエラーが検出された場合、ダウンロード制御装置１は動作不能と判断し全ての処理を停止する。

ＣＰＵ２はメモリ部３の作業領域８の割込み中継ベクタ４８を設定する（Ｓ６３）。続いて、通信インターフェース４の初期化し通信インターフェース４からの割込みを許可した後（Ｓ６４）、ダウンロード待ちタイマが起動される（Ｓ６５）。

ＣＰＵ２は、ダウンロード待ちタイマがタイムアウトするまでに上位制御装置からダウンロード開始コマンドを受信した場合（Ｓ６６，Ｓ６７）、図８を参照して後に詳述するダウンロードモジュールファイル２０のダウンロード処理を実行する（Ｓ６８）。このダウンロード処理の結果、エラーが生じた場合は処理を停止し、正常であった場合は手順Ｓ６０に戻る（Ｓ６９）。

上記手順Ｓ６６において、ＣＰＵ２がダウンロード待ちタイマのタイムアウトを検出した場合、ダウンロードの待ち状態を終了し、図７に示す処理に移行する。

ＣＰＵ２はダウンロード部７の内容を検査し、ダウンロード完了状態であるか、初期状態であるか、それ以外の不正なエラー状態であるかを判定する（図７中の処理手順Ｓ７０）。この検査は例えばダウンロード部７の特定の番地に予め定められた状態コードが書き込まれているか否かで判定する。

ＣＰＵ２は、ダウンロード完了状態である場合、さらにダウンロード部７のデータから計算したチェックサムとダウンロード部チェックディジット４７とを比較して、ダウンロード部７内の内容が正しい状態にあることを確認する（Ｓ７１，Ｓ７２）。

ダウンロード部７の内容が正しい状態にあれば、ダウンロード部７のダウンロード部コード４６が実行可能であると判断し、ダウンロード部コード４６へジャンプする（Ｓ７３）。

ＣＰＵ２は全ての割込みデバイスを停止した後（Ｓ７４）、作業領域８の割込み中継ベクタ４８を設定する（Ｓ７５）。続いて、ＣＰＵ２は初期設定の後（Ｓ７６）、装置の基本機能の処理に移行する（Ｓ７７）。

ＣＰＵ２は、手順Ｓ７１で初期状態または不正プログラムデータであることを検出した場合、または手順Ｓ７３でエラーを検出した場合は、初期化待ちタイマーを起動し（Ｓ７８）、タイムアウトになったとき（Ｓ７９）、ダウンロード部７のコード４６及びチェックディジット４７を初期化する。つまり、ローダ部６のダウンロード部初期コード４４をダウンロード部７に展開する（Ｓ８０）。

ダウンロード処理ルーチンを示す図８においては、ＣＰＵ２は通信回線５及び通信インターフェース４を通して上位制御装置から暗号化されたダウンロードモジュールファイル２０（図３参照）のヘッダ部２１を受信して、メモリ部３の作業領域８に格納した後、ヘッダ部２１のプログラムモジュール識別情報２３をチェックする。ＣＰＵ２は、受信データエラーがなければ、受信したダウンロードモジュールファイル２０のヘッダ部２１をチェックする（処理手順Ｓ８１，Ｓ８２）。

正当なダウンロードモジュールファイル２０である場合、復号用暗号鍵が生成

される（Ｓ８３）。この復号用暗号鍵は実行プログラム格納領域（ダウンロード部）７の特定アドレスに既に格納されている旧プログラムデータと、受信したファイル２０のヘッダ部２１の一部のデータとから生成される。ここでは、ヘッダ部２１の一部のデータとして、プログラムモジュール識別情報２３のうちのモジュール名称、モジュール作成日付及びモジュール版数を利用する。

次に、ＣＰＵ２はファイル２０のデータ部２２の第１の本体部を受信して復号し（Ｓ８４）、復号化した格納開始アドレスとデータ長とが正常値であるか否かを判断する（Ｓ８５）。

正常値である場合、復号化されたデータ部２２のチェックディジットが算出される。ＣＰＵ２は、算出したデータ部２２のチェックディジットと、受信したファイル２０のデータ部２２中のチェックディジットとが、一致するか否かを判断する（Ｓ８６）。

チェックディジットが一致し、データ部２２の最初の本体部である場合は、メモリ部３のダウンロード部７が初期状態にクリアされる（Ｓ８７、Ｓ８８）。ＣＰＵ２は、最初の本体部ではないと判断した場合、またはダウンロード部７をクリアした後、メモリ部３の作業領域８に格納している受信プログラムデータを実行プログラム格納領域７に書き込む（Ｓ８９）。

ＣＰＵ２はデータ部２２の最後の本体部を受信してプログラムデータを実行プログラム格納領域７に書き込むまで、上記手順Ｓ８４からＳ８９の処理を繰り返して行う（Ｓ９０）。

［変形例］

なお、データサイズの変化しないＤＥＳ－ＣＢＣ暗号処理の代わりに、データ圧縮処理、またはデータ圧縮処理及び暗号処理の組み合わで、プログラムデータを処理してもよい。つまり、暗号化アルゴリズムとして、可逆データ圧縮アルゴリズムや、可逆データ圧縮アルゴリズムと暗号化アルゴリズムとを組み合わせたアルゴリズムを用いる。データ圧縮により、通信データ量が減少し、ダウンロード所要時間を短縮できるだけではなく、アルゴリズムが複雑になり、不正目的のダウンロードモジュールの解読がより困難になる。

また、ハッシュ関数に基づくハッシュ技法を用いて、暗号鍵のデータサイズよ

りも大きなプログラムデータの一部または全体及び識別情報の一部または全体から暗号鍵を生成してもよい。これにより、プログラムデータや識別情報において、変更されても検出できない部分を減少できる。

上述した実施の形態における処理はコンピュータで実行可能なプログラムとして提供され、ＣＤ－ＲＯＭやフロッピーディスクなどの記録媒体、さらには通信回線を経て提供可能である。

産業上の利用可能性

以上説明したように、本発明によれば、既にダウンロードされているプログラムデータと、これからダウンロードするモジュールの識別情報とを利用して、暗号化されたダウンロード対象のモジュールを受信することにより、プログラムデータの解読やダウンロード可能な不正プログラムの作成を困難にするとともに、誤ったダウンロードを防御することができる。

また、本発明によれば、ダウンロードが成功せず、プログラムが実行できない状態になったことを検出して自動復旧し、自動復旧までに時間を置くことにより、不正プログラムの開発を困難にすることができる。

請求の範囲

１．　制御機能を実行するための実行プログラムデータを書き換え可能な状態で格納する第１の記憶手段と；

更新対象の新たな実行プログラムデータ及びモジュール識別情報を含むダウンロードモジュールを格納する第２の記憶手段と；

前記第１の記憶手段に格納されている前記実行プログラムデータと同一のプログラムデータと、前記モジュール識別情報とから作成された暗号鍵によって暗号化された前記ダウンロードモジュールを受信して前記第２の記憶手段に格納する第１の制御手段と；

前記第１の記憶手段内の前記実行プログラムデータのデータと、前記第２の記憶手段内の前記ダウンロードモジュールのデータとから作成した暗号鍵によって前記ダウンロードモジュールを復号化し、前記ダウンロードモジュール中に暗号化されている格納開始アドレス、データ長及びチェックディジットが正当な値に平文化された場合、復号化された前記新たな実行プログラムデータで前記第１の記憶手段内の前記実行プログラムデータを置き換える第２の制御手段と；

を備えるダウンロード機能を有する制御装置。

２．　ダウンロード機能を起動後、予め定めた一定時間のみ、前記新たな実行プログラムデータを含む前記ダウンロードモジュールを受信可能とする第３の制御手段を更に備える

請求項１記載のダウンロード機能を有する制御装置。

３．　前記ダウンロードモジュールの受信ができなくなった状態で特定のリセットコマンドを受信した場合、前記ダウンロード機能を再起動し、前記新たな実行プログラムデータを含む前記ダウンロードモジュールを受信可能とする第４の制御手段を更に備える

請求項２記載のダウンロード機能を有する制御装置。

４．　前記ダウンロード機能の起動時に最初に実行され、前記第２の記憶手段に

前記ダウンロードモジュールを格納するとともに、前記第１の記憶手段に格納された前記制御機能の実行プログラムデータを実行するローダを格納する第３の記憶手段を更に備える

請求項２または３記載のダウンロード機能を有する制御装置。

５．　前記ローダが前記第１の記憶手段内の前記実行プログラムデータの全データに基づく演算結果から得られるチェックディジット値と、前記第１の記憶手段内の前記実行プログラムデータの特定アドレスのデータとが一致した場合、前記第１の記憶手段内の前記実行プログラムデータを実行可能とする第５の制御手段を更に備える

請求項４記載のダウンロード機能を有する制御装置。

６．　前記ローダが格納されている前記第３の記憶手段に、前記第１の記憶手段に格納して実行可能な実行プログラムデータを格納しておき、

前記ローダが起動されて前記第１の記憶手段内の前記実行プログラムデータをチェックした結果、この実行プログラムデータを実行できないと判断した場合、前記第３の記憶手段内の前記ローダ所有の前記実行プログラムデータを前記第１の記憶手段に格納して前記制御機能を回復する第６の制御手段を更に備える

請求項５記載のダウンロード機能を有する制御装置。

７．　前記ローダが起動されて前記第１の記憶手段内の前記実行プログラムデータをチェックした結果、この実行プログラムデータを実行できないと判断した場合、前記第１の記憶手段を既知の状態に初期化して前記新たな実行プログラムデータの格納を可能にする第７の制御手段を更に備える

請求項５記載のダウンロード機能を有する制御装置。

８．　前記ローダ所有の前記実行プログラムデータを前記第１の記憶手段に格納するまでの待ち合わせ時間を設定し、前記ローダによる前記第１の記憶手段の初期化と不正な実行プログラムデータを含む前記ダウンロードモジュールの前記第

２の記憶手段への格納との繰り返しを制限する第８の制御手段を更に備える

請求項６記載のダウンロード機能を有する制御装置。

９．　前記ローダにより前記第１の記憶手段を初期化するまでの待ち合わせ時間を設定し、前記ローダによる前記第１の記憶手段の初期化と不正な実行プログラムデータを含む前記ダウンロードモジュールの前記第２の記憶手段への格納との繰り返しを制限する第９の制御手段を更に備える

請求項７記載のダウンロード機能を有する制御装置。

１０．　前記ダウンロードモジュールは、少なくとも前記モジュール識別情報としてのモジュール名称、モジュール作成日付及びモジュール版数と格納開始アドレスとを格納する固定長のヘッダ部と、

ブロック長とそれに対応する長さのデータとを格納する少なくとも１つのデータ部とから構成され、

前記データ部が実行プログラムデータ対応の実際のデータ長、格納開始アドレス、実行プログラムデータ、暗号化できるデータ長にするためのパッドデータ、及びこれらから生成するチェックディジットを含むブロックを暗号化されている

請求項１記載のダウンロード機能を有する制御装置。

１１．　前記第１の記憶手段内の前記実行プログラムデータのデータと、前記第２の記憶手段内の前記ダウンロードモジュールの前記モジュール識別情報のデータとから作成した暗号鍵によって前記ダウンロードモジュールを復号化する

請求項１０記載のダウンロード機能を有する制御装置。

１２．　制御機能を実行するための実行プログラムデータを書き換え可能な状態で第１の記憶手段に格納するステップと；

更新対象の新たな実行プログラムデータ及びモジュール識別情報を含むダウンロードモジュールを第２の記憶手段に格納するステップと；

前記第１の記憶手段に格納されている前記実行プログラムデータと同一のプロ

グラムデータと、前記モジュール識別情報とから作成された暗号鍵によって暗号化された前記ダウンロードモジュールを受信して前記第２の記憶手段に格納するステップと；

前記第１の記憶手段内の前記実行プログラムデータのデータと、前記第２の記憶手段内の前記ダウンロードモジュールのデータとから作成した暗号鍵によって前記ダウンロードモジュールを復号化し、前記ダウンロードモジュール中に暗号化されている格納開始アドレス、データ長及びチェックディジットが正当な値に平文化された場合、復号化された前記新たな実行プログラムデータで前記第１の記憶手段内の前記実行プログラムデータを置き換えるステップと；

を備えるダウンロード制御方法。

１３．　ダウンロード機能を起動後、予め定めた一定時間のみ、前記新たな実行プログラムデータを含む前記ダウンロードモジュールを受信可能とするステップを更に備える

請求項１２記載のダウンロード制御方法。

１４．　前記ダウンロードモジュールの受信ができなくなった状態で特定のリセットコマンドを受信した場合、前記ダウンロード機能を再起動し、前記新たな実行プログラムデータを含む前記ダウンロードモジュールを受信可能とするステップを更に備える

請求項１３記載のダウンロード制御方法。

１５．　第３の記憶手段に格納されたローダが最初に実行され、前記ダウンロード機能はこのローダが実行し、前記ダウンロード機能におけるダウンロードモジュールが受信可能であるステップが正常終了した場合に、前記第１の記憶手段に格納された前記制御機能の実行プログラムデータを実行するステップを更に備える

請求項１３または１４記載のダウンロード制御方法。

１６．　前記ローダが前記第１の記憶手段内の前記実行プログラムデータの全データに基づく演算結果から得られるチェックディジット値と、前記第１の記憶手段内の前記実行プログラムデータの特定アドレスのデータとが一致した場合、前記第１の記憶手段内の前記実行プログラムデータを実行可能とするステップを更に備える

請求項１５記載のダウンロード制御方法。

１７．　前記ローダが格納されている前記第３の記憶手段に、前記第１の記憶手段に格納して実行可能な実行プログラムデータを格納するステップと；

前記ローダが起動されて前記第１の記憶手段内の前記実行プログラムデータをチェックした結果、この実行プログラムデータを実行できないと判断した場合、前記第３の記憶手段内の前記ローダ所有の前記実行プログラムデータを前記第１の記憶手段に格納して前記制御機能を回復するステップとを更に備える

請求項１６記載のダウンロード制御方法。

１８．　前記ローダが起動されて前記第１の記憶手段内の前記実行プログラムデータをチェックした結果、この実行プログラムデータを実行できないと判断した場合、前記第１の記憶手段を既知の状態に初期化して前記新たな実行プログラムデータの格納を可能にするステップを更に備える

請求項１６記載のダウンロード制御方法。

１９．　前記ローダ所有の前記実行プログラムデータを前記第１の記憶手段に格納するまでの待ち合わせ時間を設定し、前記ローダによる前記第１の記憶手段の初期化と不正な実行プログラムデータを含む前記ダウンロードモジュールの前記第２の記憶手段への格納との繰り返しを制限するステップを更に備える

請求項１７記載のダウンロード制御方法。

２０．　前記ローダにより前記第１の記憶手段を初期化するまでの待ち合わせ時間を設定し、前記ローダによる前記第１の記憶手段の初期化と不正な実行プログ

ラムデータを含む前記ダウンロードモジュールの前記第２の記憶手段への格納との繰り返しを制限するステップを更に備える

請求項１８記載のダウンロード制御方法。

２１．　前記ダウンロードモジュールは、少なくとも前記モジュール識別情報としてのモジュール名称、モジュール作成日付及びモジュール版数と格納開始アドレスとを格納する固定長のヘッダ部と、

ブロック長とそれに対応する長さのデータとを格納する少なくとも１つのデータ部とから構成され、

前記データ部が実行プログラムデータ対応の実際のデータ長、格納開始アドレス、実行プログラムデータ、暗号化できるデータ長にするためのパッドデータ、及びこれらから生成するチェックディジットを含むブロックを暗号化されている

請求項１２記載のダウンロード制御方法。

２２．　前記第１の記憶手段内の前記実行プログラムデータのデータと、前記第２の記憶手段内の前記ダウンロードモジュールの前記モジュール識別情報のデータとから作成した暗号鍵によって前記ダウンロードモジュールを復号化するステップを更に備える

請求項２１記載のダウンロード制御方法。

要　約　書

ダウンロード機能を有する制御装置は、制御機能を実行するための実行プログラムデータを書き換え可能な状態で格納する第１の記憶手段と；更新対象の新たな実行プログラムデータ及びモジュール識別情報を含むダウンロードモジュールを格納する第２の記憶手段と；前記第１の記憶手段に格納されている前記実行プログラムデータと同一のプログラムデータと、前記モジュール識別情報とから作成された暗号鍵によって暗号化された前記ダウンロードモジュールを受信して前記第２の記憶手段に格納する第１の制御手段と；前記第１の記憶手段内の前記実行プログラムデータのデータと、前記第２の記憶手段内の前記ダウンロードモジュールのデータとから作成した暗号鍵によって前記ダウンロードモジュールを復号化し、前記ダウンロードモジュール中に暗号化されている格納開始アドレス、データ長及びチェックディジットが正当な値に平文化された場合、復号化された前記新たな実行プログラムデータで前記第１の記憶手段内の前記実行プログラムデータを置き換える第２の制御手段とを備える。

FIG. 1

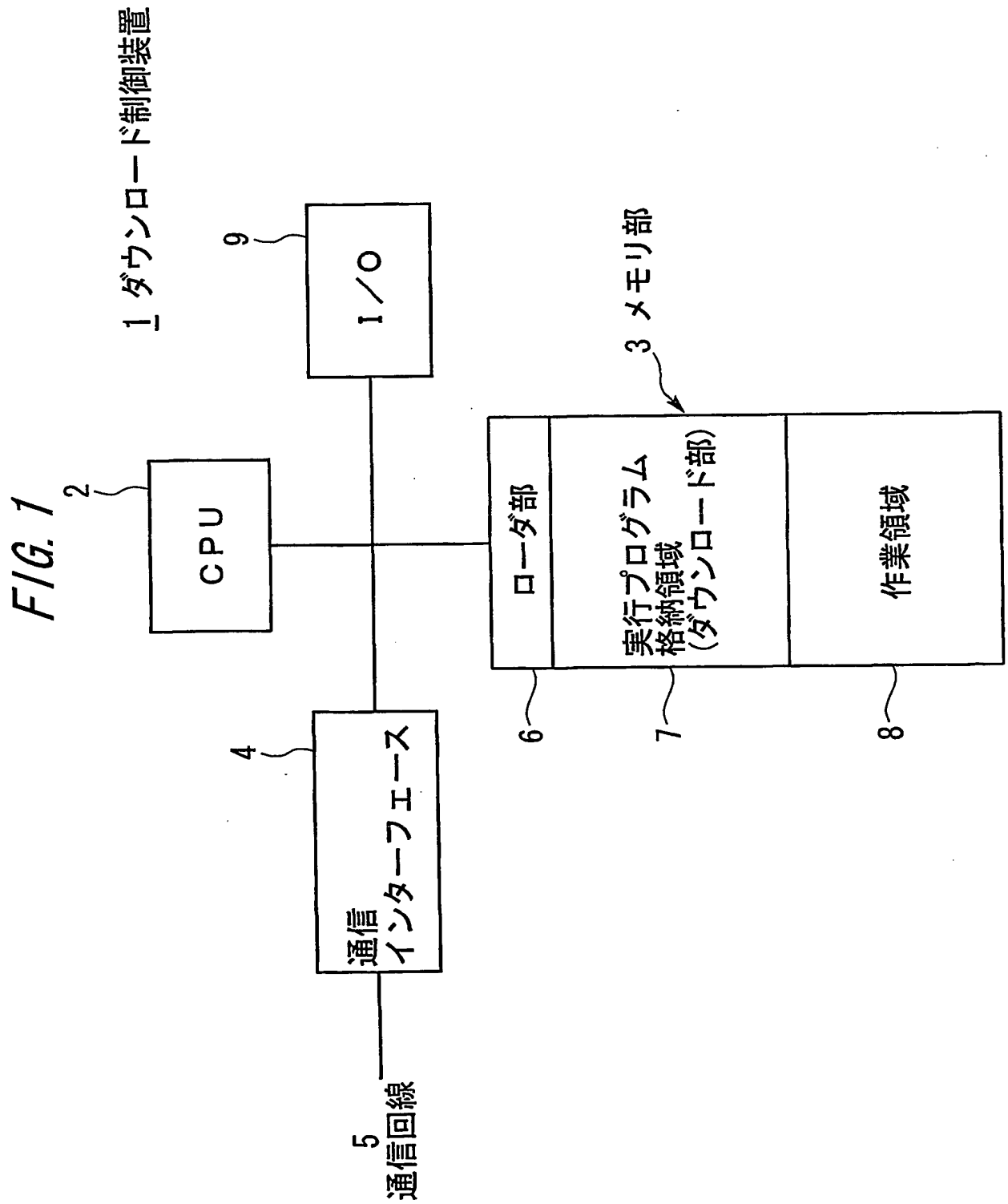

1 ダウンロード制御装置
2
CPU
9
I／O
3 メモリ部
ローダ部
実行プログラム
格納領域
(ダウンロード部)
作業領域
6
7
8
4
通信
インターフェース
5
通信回線

FIG. 2

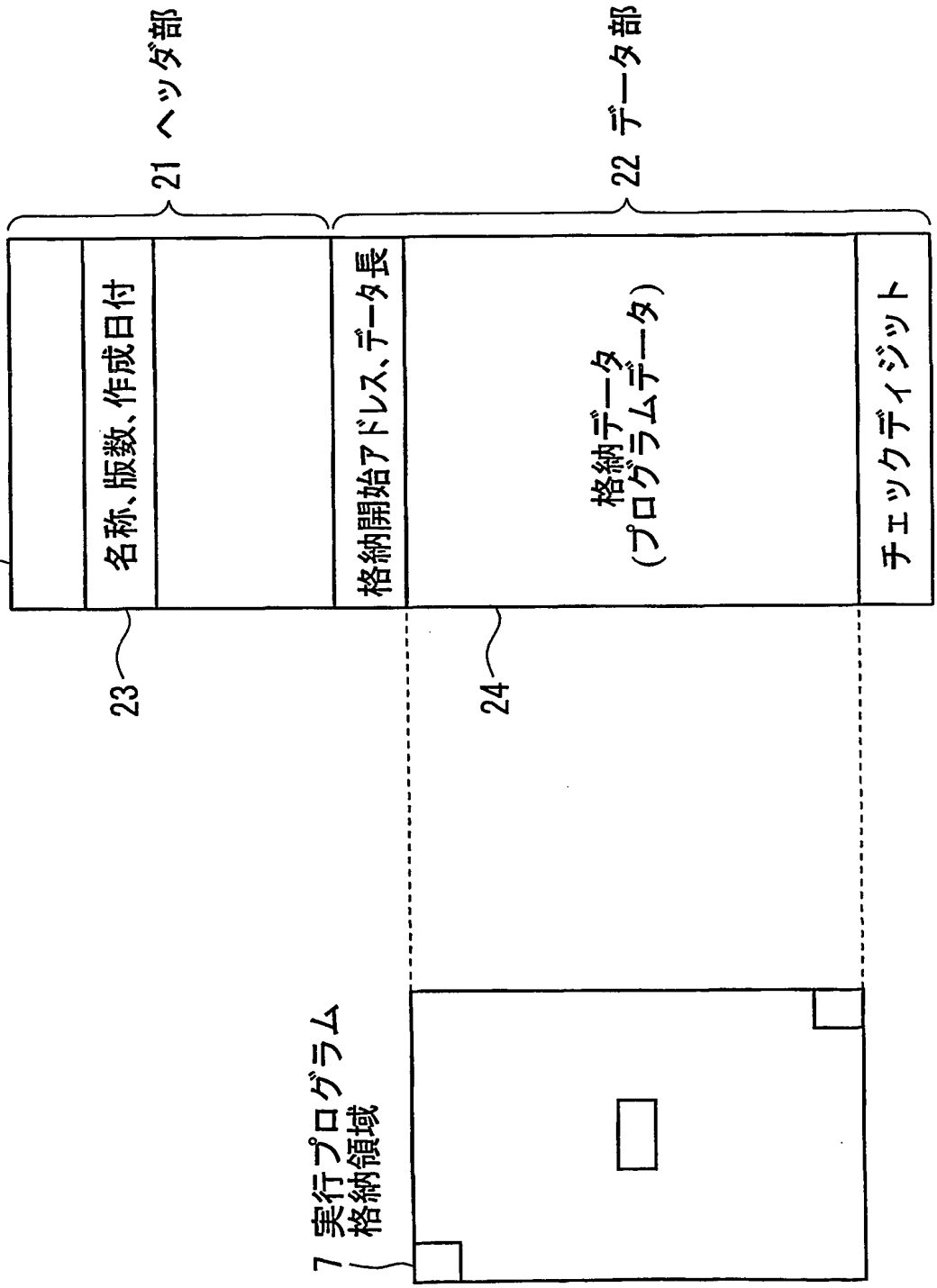

20 ダウンロード
モジュールファイル
21 ヘッダ部
22 データ部
名称、版数、作成日付
格納開始アドレス、データ長
格納データ
(プログラムデータ)
チェックディジット
23
24
7 実行プログラム
格納領域

FIG. 3

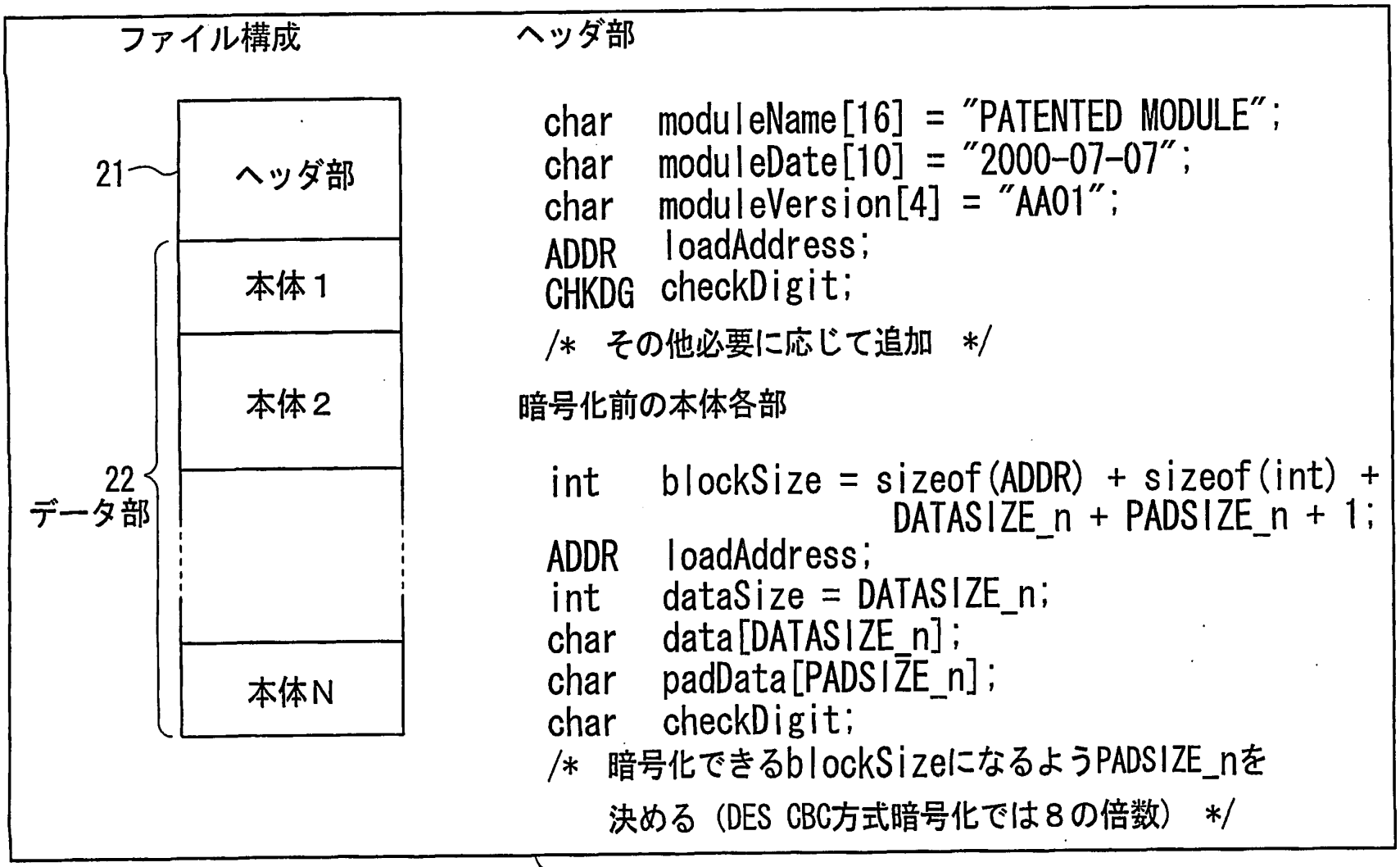

ファイル構成
ヘッダ部
21
ヘッダ部
本体１
本体２
22
データ部
本体N
char moduleName[16] = "PATENTED MODULE";
char moduleDate[10] = "2000-07-07";
char moduleVersion[4] = "AA01";
ADDR loadAddress;
CHKDG checkDigit;
/* その他必要に応じて追加 */
暗号化前の本体各部
int blockSize = sizeof(ADDR) + sizeof(int) +
DATASIZE_n + PADSIZE_n + 1;
ADDR loadAddress;
int dataSize = DATASIZE_n;
char data[DATASIZE_n];
char padData[PADSIZE_n];
char checkDigit;
/* 暗号化できるblockSizeになるようPADSIZE_nを
決める（DES CBC方式暗号化では８の倍数） */
20 ダウンロードモジュールファイル

FIG. 4

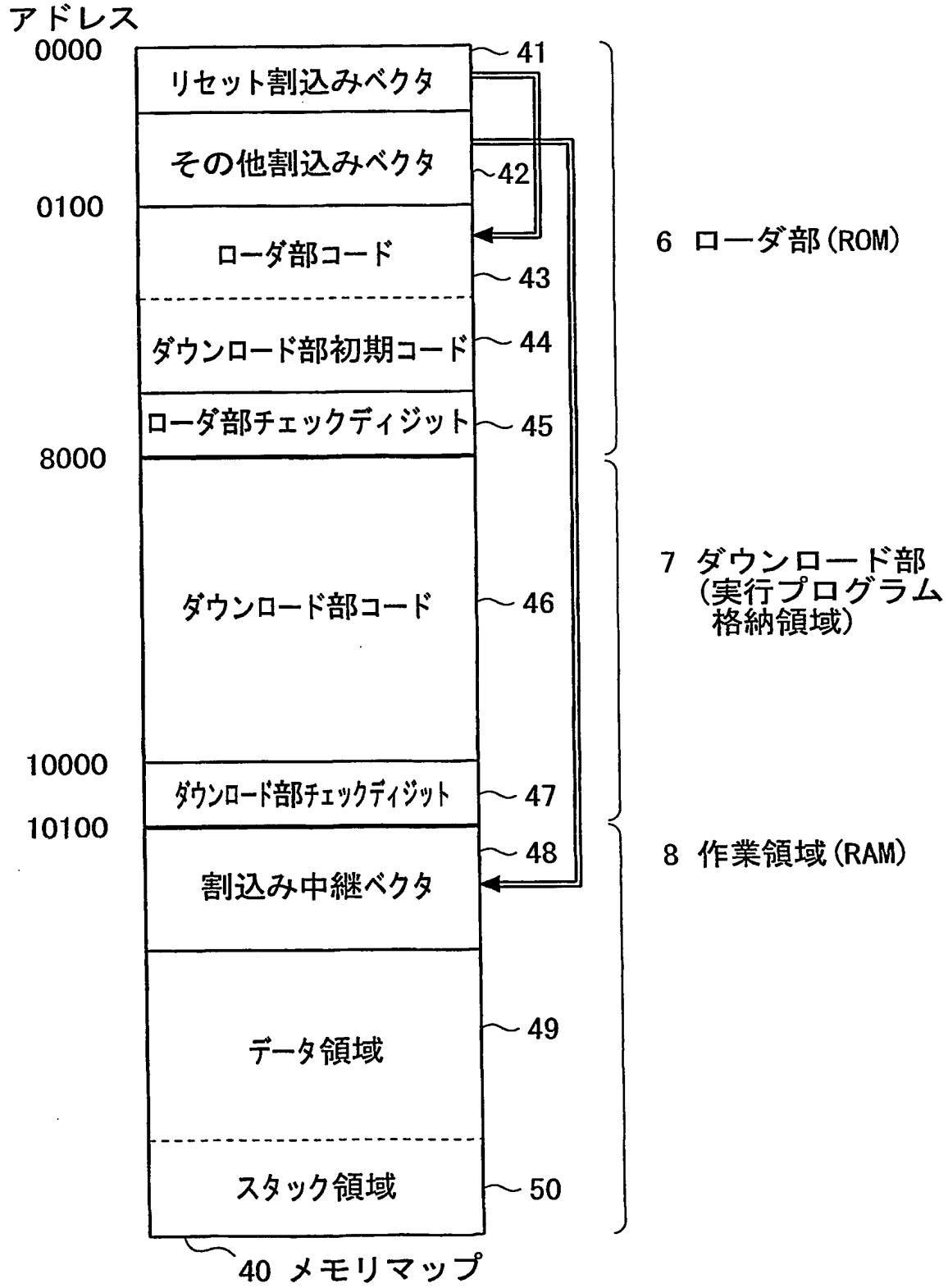

アドレス
0000
リセット割込みベクタ
41
その他割込みベクタ
42
0100
ローダ部コード
43
ダウンロード部初期コード
44
ローダ部チェックディジット
45
8000
ダウンロード部コード
46
10000
ダウンロード部チェックディジット
47
10100
割込み中継ベクタ
48
データ領域
49
スタック領域
50
40 メモリマップ
6 ローダ部(ROM)
7 ダウンロード部
(実行プログラム
格納領域)
8 作業領域(RAM)

FIG. 5

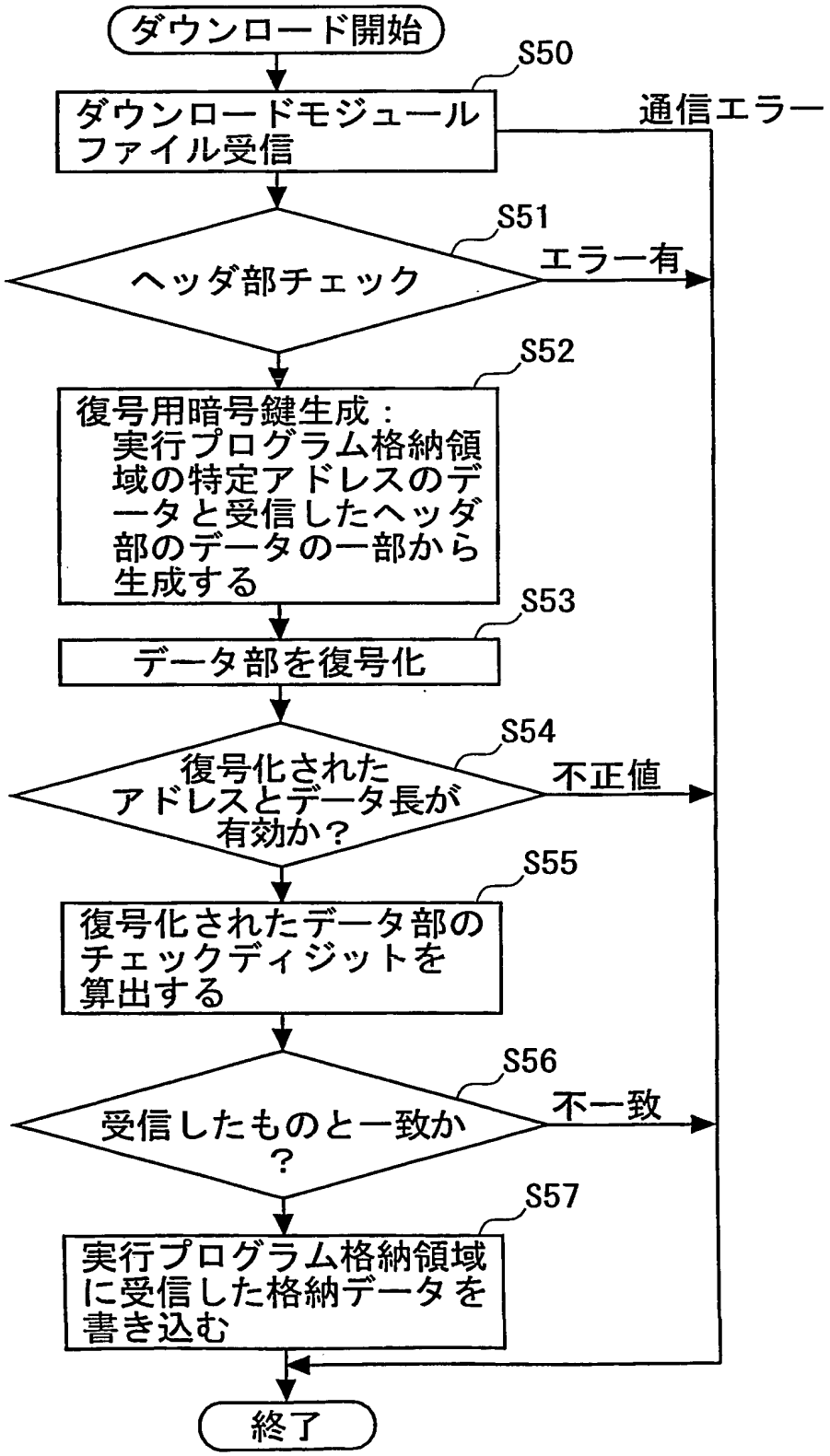

ダウンロード開始
S50
ダウンロードモジュールファイル受信
通信エラー
S51
ヘッダ部チェック
エラー有
S52
復号用暗号鍵生成：実行プログラム格納領域の特定アドレスのデータと受信したヘッダ部のデータの一部から生成する
S53
データ部を復号化
S54
復号化されたアドレスとデータ長が有効か？
不正値
S55
復号化されたデータ部のチェックディジットを算出する
S56
受信したものと一致か？
不一致
S57
実行プログラム格納領域に受信した格納データを書き込む
終了

FIG. 6

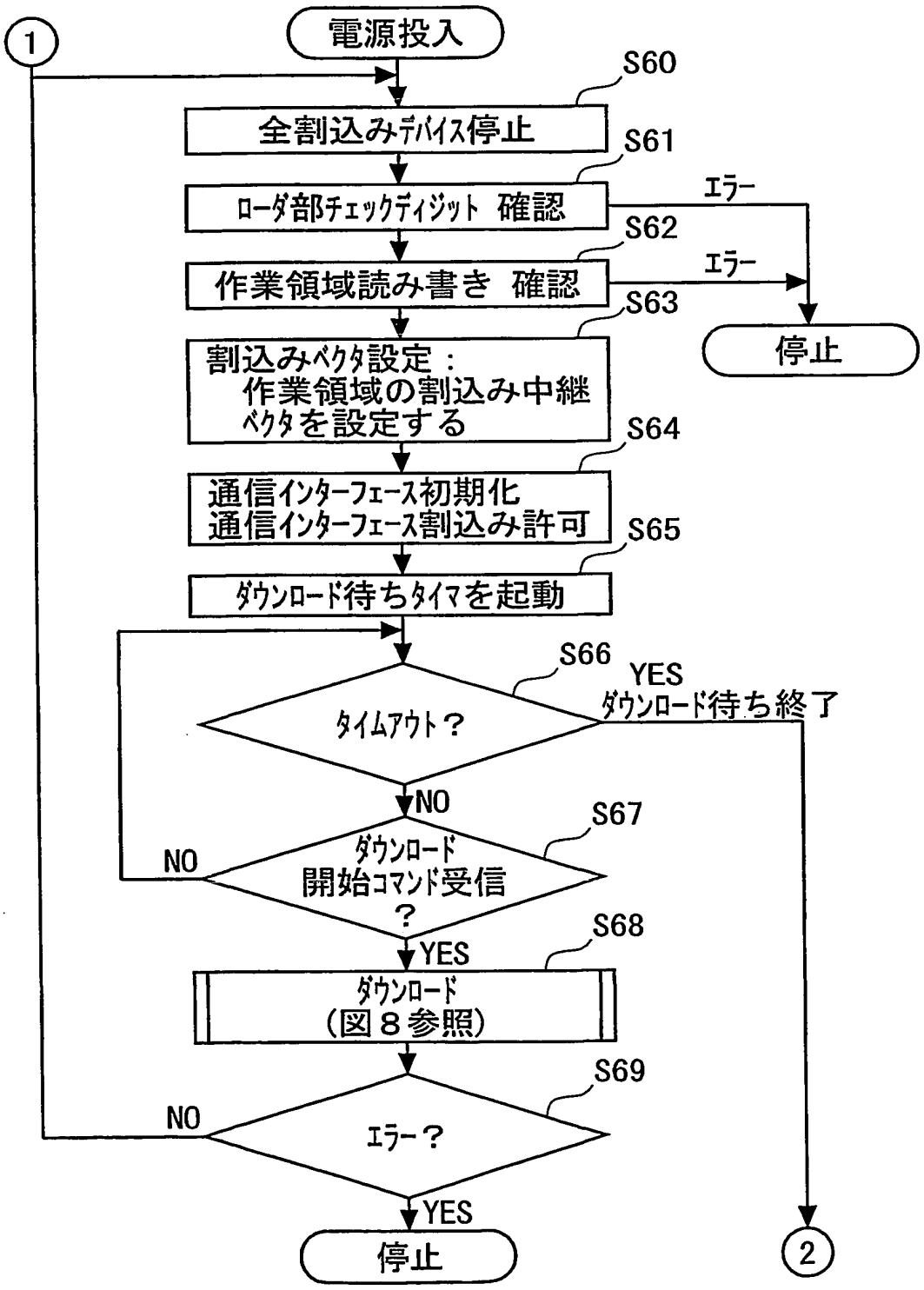

①
電源投入
S60
全割込みデバイス停止
S61
ローダ部チェックディジット 確認
エラー
S62
作業領域読み書き 確認
エラー
S63
停止
割込みベクタ設定：
作業領域の割込み中継
ベクタを設定する
S64
通信インターフェース初期化
通信インターフェース割込み許可
S65
ダウンロード待ちタイマを起動
S66
タイムアウト？
YES
ダウンロード待ち終了
NO
S67
ダウンロード
開始コマンド受信
？
NO
YES
S68
ダウンロード
（図８参照）
S69
エラー？
NO
YES
停止
②

FIG. 7

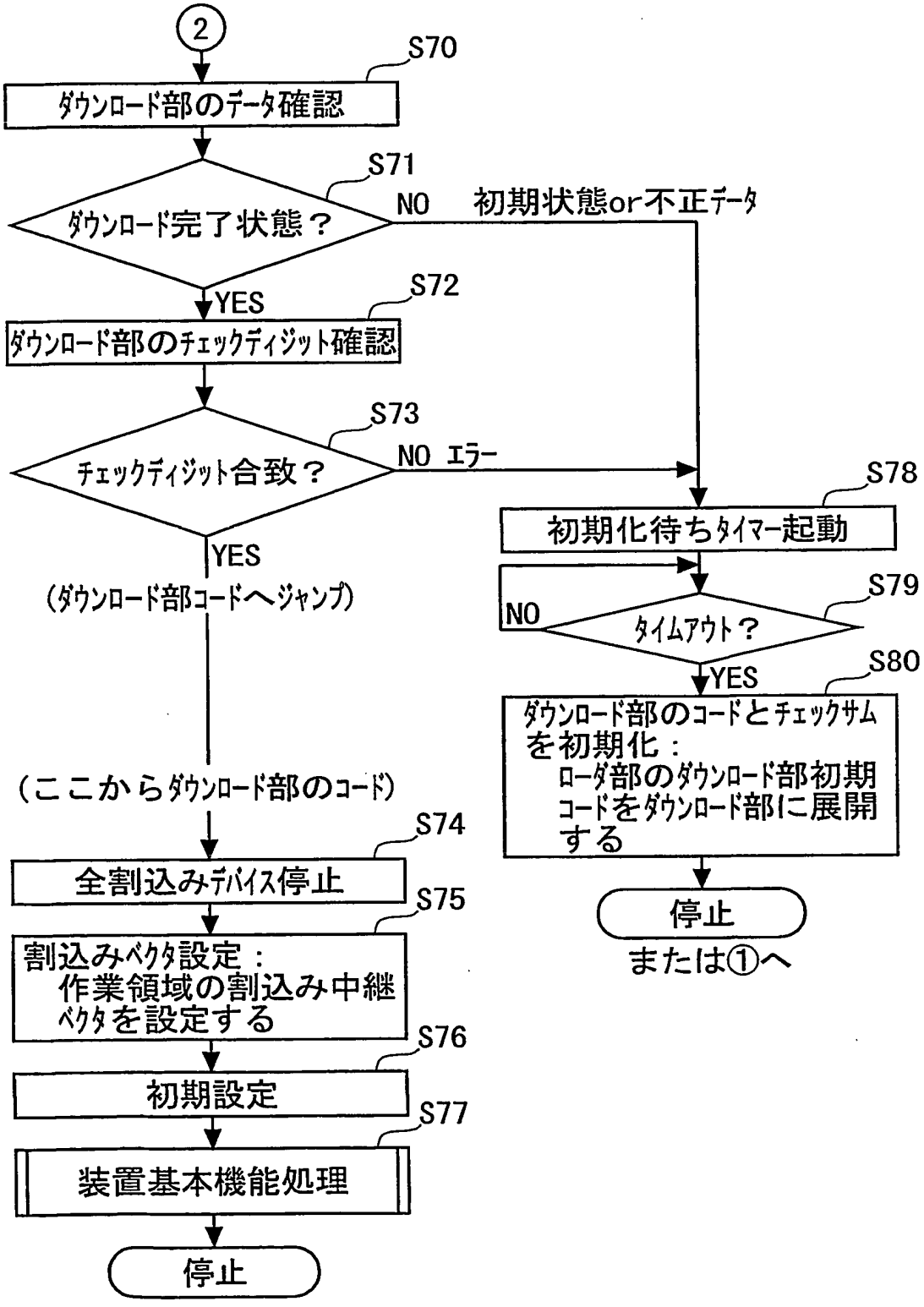
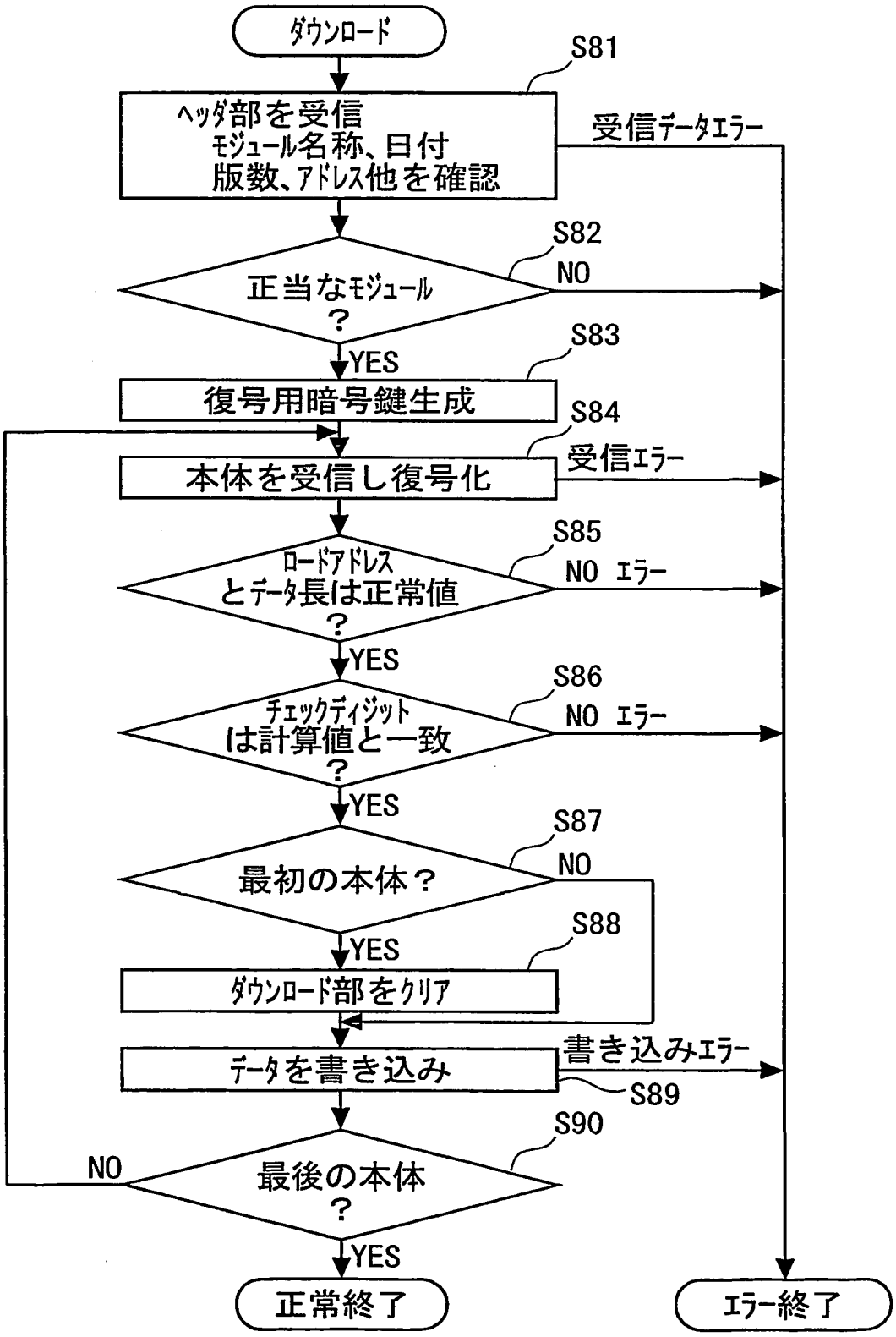

2
S70
ダウンロード部のデータ確認
S71
ダウンロード完了状態？
NO
初期状態or不正データ
YES
S72
ダウンロード部のチェックディジット確認
S73
チェックディジット合致？
NO エラー
YES
(ダウンロード部コードへジャンプ)
S78
初期化待ちタイマー起動
S79
NO
タイムアウト？
YES
S80
ダウンロード部のコードとチェックサムを初期化：
ローダ部のダウンロード部初期コードをダウンロード部に展開する
停止
または①へ
(ここからダウンロード部のコード)
S74
全割込みデバイス停止
S75
割込みベクタ設定：
作業領域の割込み中継ベクタを設定する
S76
初期設定
S77
装置基本機能処理
停止

FIG. 8


ダウンロード
S81
ヘッダ部を受信
モジュール名称、日付
版数、アドレス他を確認
受信データエラー
S82
正当なモジュール
？
NO
YES
S83
復号用暗号鍵生成
S84
本体を受信し復号化
受信エラー
S85
ロードアドレス
とデータ長は正常値
？
NO エラー
YES
S86
チェックディジット
は計算値と一致
？
NO エラー
YES
S87
最初の本体？
NO
YES
S88
ダウンロード部をクリア
書き込みエラー
データを書き込み
S89
S90
NO
最後の本体
？
YES
正常終了
エラー終了

名義変更届

特許庁長官　　殿

10.12.02

1．国際出願の表示　　ＰＣＴ／ＪＰ０１／００３５６

2．出　願　人

名　称　　富士通株式会社
ＦＵＪＩＴＳＵ　ＬＩＭＩＴＥＤ

あて名　　〒２１１－８５８８
日本国神奈川県川崎市中原区上小田中４丁目１番１号
１－１，Ｋａｍｉｋｏｄａｎａｋａ　４－ｃｈｏｍｅ，
Ｎａｋａｈａｒａ－ｋｕ，Ｋａｗａｓａｋｉ－ｓｈｉ，
Ｋａｎａｇａｗａ　２１１－８５８８　ＪＡＰＡＮ

国　籍　　日本国　Ｊａｐａｎ

住　所　　日本国　Ｊａｐａｎ

3．届出の内容　　新名義人

事件との関係　　米国を除く全ての指定国における出願人

名　称　　富士通株式会社
ＦＵＪＩＴＳＵ　ＬＩＭＩＴＥＤ

あて名　　〒２１１－８５８８
日本国神奈川県川崎市中原区上小田中４丁目１番１号
１－１，Ｋａｍｉｋｏｄａｎａｋａ　４－ｃｈｏｍｅ，
Ｎａｋａｈａｒａ－ｋｕ，Ｋａｗａｓａｋｉ－ｓｈｉ，
Ｋａｎａｇａｗａ　２１１－８５８８　ＪＡＰＡＮ

国　籍　　日本国　Ｊａｐａｎ

住　所　　日本国　Ｊａｐａｎ

事件との関係　　米国を除く全ての指定国における出願人

名　称　　富士通フロンテック株式会社
ＦＵＪＩＴＳＵ　ＦＲＯＮＴＥＣＨ　ＬＩＭＩＴＥＤ

あて名　　〒２０６－８５５５
日本国東京都稲城市矢野口１７７６番地
１７７６，Ｙａｎｏｋｕｃｈｉ，Ｉｎａｇｉ－ｓｈｉ，
Ｔｏｋｙｏ　２０６－８５５５
ＪＡＰＡＮ

国　籍　　日本国　Ｊａｐａｎ

住　所　　日本国　Ｊａｐａｎ

事件との関係　指定国米国における出願人及び
すべての指定国における発明者

氏　名　柏田　猛
KASHIWADA, Takeshi
あて名　〒211－8588
日本国神奈川県川崎市中原区上小田中４丁目１番１号
富士通株式会社内
C／O FUJITSU LIMITED
1－1, Kamikodanaka 4－chome,
Nakahara－ku, Kawasaki－shi,
Kanagawa 211－8588 JAPAN
国　籍　日本国　Japan
住　所　日本国　Japan

4．代理人

氏　名　（８９２４）　弁理士　遠　山　勉
TOYAMA Tsutomu
あて名　〒１０３－０００４　日本国東京都中央区東日本橋３丁目
４番１０号ヨコヤマビル６階
Yokoyama Building 6th floor,
4－10, Higashi Nihonbashi 3－chome,
Chuo－ku, Tokyo
103－0004 JAPAN

氏　名　（９０５１）　弁理士　松　倉　秀　実
MATSUKURA Hidemi
あて名　〒１０３－０００４　日本国東京都中央区東日本橋３丁目
４番１０号ヨコヤマビル６階
Yokoyama Building 6th floor,
4－10, Higashi Nihonbashi 3－chome,
Chuo－ku, Tokyo
103－0004 JAPAN

5．添付書類の目録　（１）代理権を証明する書面　１通
（包括委任状の写し）